HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 109 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, May 29, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, May 29, 2018

● (0850)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): Good morning, everybody, and welcome to the Standing Committee on Access to Information, Privacy and Ethics meeting number 109. Pursuant to Standing Order 108(3)(h)(vii), we are doing a study of breach of personal information involving Cambridge Analytica and Facebook. Today with us is Christopher Wylie, via teleconference from the U.K.

Thanks for coming, Mr. Wylie.

Have you been made aware that you're going to be sworn in today?

Mr. Christopher Wylie (As an Individual): Yes.

The Chair: Okay, so we're going to do that right now.

Mr. Christopher Wylie: I, Christopher Wylie, do solemnly, sincerely, and truly affirm and declare the taking of any oath is according to my religious belief unlawful; and I do solemnly, sincerely, and truly affirm and declare that the evidence that I shall give on this examination shall be the truth, the whole truth, and nothing but the truth.

The Chair: Thank you, Mr. Wylie. It's unfortunate that you couldn't be with us today, but we understand you're testifying in the U.K. on the current case that's before Parliament in the U.K. We appreciate it. It would have been nice to have you here, but we realize your obligation is over in the U.K.

Would you like to have any opening comments, Mr. Wylie?

Mr. Christopher Wylie: No. I'm happy to take questions.

The Chair: We'll start off. The first question goes to Mr. Erskine-Smith, for seven minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much, Mr. Wylie.

First, just a short question is, can you confirm how long you worked for Cambridge Analytica?

Mr. Christopher Wylie: Yes. Does your question have to do with Cambridge Analytica precisely, or are you talking also about SCL Group?

Mr. Nathaniel Erskine-Smith: Both.

Mr. Christopher Wylie: I was the director of research. I started my engagement in July 2013 with SCL Group, and I completed that engagement around the end of October or November 2014.

Mr. Nathaniel Erskine-Smith: I have a couple of quick confirmations. By the way, when I say Cambridge Analytica or SCL, I'm going to refer to them both together. Cambridge Analytica/SCL worked on the Brexit campaign for Vote Leave and related campaigns, and in the U.S. election on behalf of President Trump. Is that correct?

Mr. Christopher Wylie: Yes. To my understanding, yes.

Mr. Nathaniel Erskine-Smith: To your knowledge, these campaigns used the information improperly collected by Kogan from Facebook users.

Mr. Christopher Wylie: I did not work on the Trump campaign, so I cannot speak specifically to what specific data was used or not used on the Trump campaign. What I can say is that the foundational modelling and data assets of Cambridge Analytica were derived from the Kogan dataset that you're referring to.

Mr. Nathaniel Erskine-Smith: We had Chris Vickery start us off here at our committee. He indicated there was this master dataset that included a number of different points of information, from U.S. election lists to the RNC trust. He even referenced the Koch brothers. We have one example that really was the foundation for why we started this study, which was of Cambridge Analytica improperly collecting information through Kogan from Facebook. Do you have other examples that you can point to of improper collection of personal information by Cambridge Analytica or SCL?

Mr. Christopher Wylie: The most concerning misappropriation of information relates to Facebook data in the United States. However, I am also aware that in other countries the company, whether it was under the auspices of SCL Group or under the auspices of Cambridge Analytica, did attempt to misappropriate other datasets. To be clear, those datasets weren't necessarily Facebook or social media datasets, those could have been government records or private company records, for example. To give you an example, my understanding is that in Trinidad there was an attempt to procure online browsing histories of citizens—

● (0855)

Mr. Nathaniel Erskine-Smith: The idea is to compile all this information from as many sources as possible into one master dataset.

Mr. Christopher Wylie: Yes. That's what you call the database of record, or the DBOR.

The idea of a DBOR is to create what you would call a "single citizen view" or a "single customer view".

The more information you have from different contacts about a person, the more you are able to accurately infer their behaviour. If you have a dataset that shows their consumer behaviour, you're able to predict certain facets of that person. If you also have online data, whether it's social media data, clickstream data, or cookie data, you're able to see another facet of that person, etc.

The idea of a DBOR is to create a holistic view of a person so you can more accurately predict different facets of their behaviour.

Mr. Nathaniel Erskine-Smith: Mr. Vickery suggested that there were very personal aspects of people's lives. The example he pointed to was leading a Biblical life, whatever that might mean. That was a way people were tagged.

In your view, what's the most personal information you saw in these databases that was acted upon?

Mr. Christopher Wylie: It depends on the definition of "most personal". I guess it's relative to what each person considers most personal.

To give you some examples of things I think most people would consider highly personal: religious views, sexual orientation, even the fact that the wider datasets were being used to infer attributes in people related to their psychological disposition, which they may or may not have known or wanted to be inferred. If you are inferring, for example, some sort of psychological neurosis in a person, that may feel very sensitive and very personal, even if that data wasn't necessarily collected as such but rather inferred from the other data that was collected.

The issue is not just what direct observations were acquired in datasets but also how less intimate observations can be transformed into inferred information about things that would be quite personal.

Mr. Nathaniel Erskine-Smith: You mentioned that it could be used for a range of different purposes. To a large degree at this committee, we've been dealing with political purposes. The information you saw collected for a range of different purposes, including from political parties, perhaps was put into this master database. Was information collected for political purposes or from election lists used for commercial purposes?

Mr. Christopher Wylie: When I was there, the primary focus after the Mercers and Steve Bannon took over was for political purposes. I know there was planning to do commercial projects, and I believe the company subsequently did perform commercial work for various companies. To be clear, I didn't work specifically on commercial projects, simply for a company itself.

Mr. Nathaniel Erskine-Smith: My last question is in relation to custom audiences. Just practically, for the sake of Canadians but also our committee, when you have this personal information about people and you want to target people, presumably you are creating a custom audience and then uploading that custom audience to advertise to that custom audience. Perhaps explain the mechanics of how this works.

Mr. Christopher Wylie: A custom audience is what Facebook would call a list of particular people who have been identified externally to create your target universe. Essentially there are a few ways to target on Facebook.

One is using Facebook's own targeting applications, for example, picking different likes that you want to target, or wanting to target people in Alberta but not Saskatchewan, that kind of thing. That doesn't involve specific lists of people. It just involves attributes, and then Facebook pulls people who match the attribute. In that process, you don't engage what is called PII, personally identifiable information.

The other way you can target ads on Facebook and other sites like Facebook is through custom audiences. This is where you have a list of people, for whatever reason, whether it's because of an algorithm or simply because of an observed attribute you want to target. You upload a list of specific individuals from your own database into Facebook, and then Facebook targets only those individual people. That directly involves the management of PII.

● (0900)

The Chair: Thank you, Mr. Erskine-Smith.

Next up for seven minutes is Mr. Kent.

Hon. Peter Kent (Thornhill, CPC): Thank you, Mr. Chair.

It's good that you could be with us here today, Mr. Wylie. You are certainly a whistle-blower of some note, and your comments a couple of months ago, saying "It is extremely uncomfortable to consider that our democracy may have been corrupted", have resonated and sparked investigations like that of our committee today. I would also note that over the years you have been a participant—an architect, if you will—of the dark art of psychographic micro-targeting and, I think, in some ways comparable to the arsonist who sets the blaze and then calls the fire department.

On January 2, 2016, you sent an email to Mr. Cummings, who you had briefed on the Leave project—the Brexit vote, the referendum in the U.K.—and followed up asking for an early meeting to consider the proposal you made, again, as you said, your in-depth technical briefing on psychographic micro-targeting. However, you also said in that email to Mr. Cummings, "Some of us will be in Ottawa this month"—January 2016—"working on a similar project for a major Canadian political party." We know now that this was the Liberal Party of Canada, and I'll come back to that later on in my questions over the next couple of hours.

I'd like to go back a decade, though, and just establish a little bit of ground information. Is it correct that you worked in the office of the Liberal leader under Stéphane Dion and Michael Ignatieff between 2007 and 2009 and launched a project that was described as "information management"?

Mr. Christopher Wylie: I worked for the office of the Leader of the Opposition, and my role in the time frame you mentioned was to look at ways of using information technologies to better engage and communicate with constituents and manage constituent information.

Hon. Peter Kent: Is it true, then, that your contract was cancelled at the direction of leader Ignatieff because he considered your work to be too invasive of Canadians' privacy?

Mr. Christopher Wylie: That is news to me. If that happened, I never heard about it. I don't believe that's true.

Hon. Peter Kent: Well, The Canadian Press quoted a Liberal insider, saying that you were "pushing a fledgling form of...data-harvesting" techniques, but Liberal officials then backed off because they didn't want to have anything to do with what they considered to be potentially too invasive.

Mr. Christopher Wylie: I don't know who this Liberal insider is, so it's hard for me to comment on what exactly they're referring to.

When I worked with the opposition leader's office, the project was primarily infrastructural. At the time, the opposition caucus did not have a coherent constituency casework management system. I think that managing casework is a legitimate activity for members of Parliament and the Leader of the Opposition to engage in, and I think that creating technological infrastructure to help them respond to the constituents more promptly is a perfectly legitimate exercise to engage in.

To the point you made, to my recollection, I was never terminated because of some kind of privacy issue. I'm not sure where you're getting that information, but I don't believe it's true.

● (0905)

Hon. Peter Kent: In this case it was from The Canadian Press, but *The Globe and Mail* reported that as "a Liberal volunteer and researcher" you "played a role in introducing and shaping the party's drive toward data-driven techniques." This gentleman—again, this volunteer—said that you were using "fringe techniques", using

> a now widely used piece of software, known as "Liberalist"—while aggressively avowing to the party's old guard that only technology could reverse the [Liberal] party's electoral fortunes.

Did you advise the Liberal Party?

Mr. Christopher Wylie: "Liberalist" is just a brand name for the CRM technology that was being developed. The thing that I would say is that just because data....

One thing that I would just caution, for anyone looking at this issue, is that the use of information in and of itself is not inherently nefarious. Every party in Canada uses a CRM system. Every party collects data. At the time, the Conservative Party had much more advanced technology and data collection infrastructure than the Liberal Party. In order to keep up with the modernization of politics, one thing that the Liberal Party at the time prioritized was setting up a CRM system to manage relationships with voters and, on the caucus side, to manage relationships with constituents. That in itself is not nefarious. That in itself is not illegal or unethical. Every party collects the electoral register in Canada and collects information on constituents or voters.

Hon. Peter Kent: Absolutely, every party does collect data. It's a matter of how much data they collect and how they use it.

Let's come back to this email that you sent at the time you were pitching the Leave vote psychographic micro-targeting. You wrote, "Some of us will be in Ottawa this month working on a similar project for a major Canadian political party". Were you pitching, basically, this same approach to the Liberal Party of Canada in January 2016?

Mr. Christopher Wylie: Let me be clear. First of all, if you read through the documentation that was sent to Dominic Cummings, nothing in there is illegal, and nothing in there is necessarily comparable to, for example, Cambridge Analytica. There was no proposal to misappropriate data.

If you collect data with awareness and consent, then that is a legitimate use and collection of data. The thing that I would just caution, again, is that simply because data is involved in a project does not mean that there is any nefarious intent or purpose for that project.

With relation to the—

The Chair: Thank you.

We'll come back.

Next up for seven minutes is Mr. Angus.

Mr. Charlie Angus (Timmins—James Bay, NDP): Thank you, Mr. Wylie, for joining our committee today.

I'm very interested in the structure of SCL. We're trying to figure out SCL, Cambridge Analytica, and AggregateIQ. When I look at SCL, I see that it was involved in psychological warfare, rumour campaigns.... It was paid by NATO. It was working around the world. Then it seems to have morphed into this election machine. Can you explain the structure of SCL to us?

● (0910)

Mr. Christopher Wylie: Sure. I believe that, in fact, some of the work that SCL was doing for NATO was actually funded by the Canadian government. Something that the committee might be interested in looking at with the Department of Defence in Ottawa is the relationship there.

In terms of the structure of SCL, it has had several iterations over time. When I was there, it was considered a group company where you had the same shareholders and board members on several different companies, which shared the same name, SCL, and then each of the companies within the group company specialized in a different area of work. The largest at the time I joined was SCL defence, so the majority of the work that SCL Group did was defence related. You also had SCL Elections, which was a much smaller consultancy that did elections work, usually in developing countries. SCL Social did work that usually didn't fit into either defence or politics. For example, if you had a health care project, that might be SCL Social. As well, SCL Commercial did commercial projects.

When Cambridge Analytica was set up, the formal relationship that it had when the intellectual property was transferred was from SCL Elections to Cambridge Analytica, so Cambridge Analytica was set up in the United States. It acquired not SCL Elections itself, but merely the intellectual property of SCL Elections, so SCL Elections assigned its IP to Cambridge Analytica. Cambridge Analytica, in return, provided a licence to that same intellectual property back to SCL Elections with a second contract that guaranteed that all work from Cambridge Analytica would be performed by SCL Elections. That was the basic set-up.

I can go into more detail if you'd like, but that's—

Mr. Charlie Angus: Well, we will get there.

Brittany Kaiser testified that AggregateIQ was the exclusive digital data engineering partner of Cambridge Analytica.

Mr. Christopher Wylie: Yes.

Mr. Charlie Angus: Chris Vickery also stated that they were the digital development team.

How does AggregateIQ fit in here?

Mr. Christopher Wylie: Around the end of October or November 2013, when SCL decided to scale and prioritize development of technology solutions, I reached out to Jeff Silvester and Zack Massingham and asked if they were interested in coming and working on projects in London. Because they had new families and they were already established in Canada, it was difficult for them to move.

The arrangement was that they would set up a Canadian company. They would be able to work in Canada. The front-facing brand would still be SCL, or SCL Canada, but they were able to remain in Canada as they worked.

AggregateIQ was set up. The first project they worked on was Trinidad. The arrangement they had with SCL was that any work that they performed for SCL would then be owned by SCL. The intellectual property that was being developed at the time was then assigned or transferred to SCL. You could think of AggregateIQ as a bit like a franchise, if you will.

Mr. Charlie Angus: Okay. We have the document., which I think were probably supplied by you, that SCL identifies Zack Massingham as head of SCL Canada.

Mr. Christopher Wylie: Yes.

Mr. Charlie Angus: There is a phone that goes to Zack Massingham as the head of SCL Canada. He said there is absolutely no connection.

Is that credible?

Mr. Christopher Wylie: No, that's completely false.

The reason AggregateIQ was set up in the first place was because there were projects that SCL was running, and then later Cambridge Analytica was running, that they needed a team of engineers to support. The arrangement was that AggregateIQ would perform that work and then exclusively license it to SCL, and then operate under the auspices of SCL Canada.

● (0915)

Mr. Charlie Angus: Why would Zack Massingham tell our committee such an obvious falsehood when there are documents? That's what we don't understand.

Mr. Christopher Wylie: I can't speak to the intentions or reasons why Zack Massingham would—

Mr. Charlie Angus: I'm sorry to interrupt. You have said that they've been very careful, technically correct in what they say, but that they use "weasel words". Why would you say that?

Mr. Christopher Wylie: The reason I said "weasel words" is because it is technically true that AggregateIQ was not part of SCL. It was a separately registered company in a separate country. However, the intellectual property licensing arrangements, the contractual arrangements, and the development work were all exclusive with SCL.

The reason I said that is because, whilst it is very technically true that AggregateIQ is a separate company, that doesn't mean that it owned the intellectual property that it was developing. SCL owned the intellectual property that it was developing.

Mr. Charlie Angus: Just to close this off, you also said that they were a proxy money-laundering operation in the Brexit, Vote Leave campaign. Did you not say that?

Mr. Christopher Wylie: When you look at the relationship that AggregateIQ had with many of the different campaign groups on the Leave side, and you see that all of those different campaign groups received donations—in some cases, very sizable donations—from Vote Leave, and that this money then all went to AggregateIQ, to me that looks like a proxy for breaking campaign spending law in the United Kingdom.

Facebook recently confirmed to The Electoral Commission and to the Parliament of the United Kingdom that in fact AggregateIQ had some of the same custom audiences and look-alike audiences that were based on their work for Vote Leave, for some of these other entities.

What has been established so far is that money went from Vote Leave to another campaign, and it then went to the same service provider for the same work that Vote Leave had. Facebook has now confirmed that some of the targeting and the target universes were exactly the same.

I don't know if calling it money laundering per se is the technically correct way of expressing that relationship, but in the general sense it does look like the relationship that it had with all of the Leave campaigns was to obfuscate electoral law in the U.K.

The Chair: Thank you, Mr. Angus.

Next up, for seven minutes, is Mr. Baylis.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Thank you, Mr. Wylie.

I'll just add a correction to what you said about the money moving from Vote Leave to one of the other ones. What we were told by AggregateIQ is that they didn't even bother passing it over. They just gave it directly to AIQ. In that sense—

Mr. Christopher Wylie: I'm sorry. You're correct. What I meant by passing the money around is that the invoices....

You are correct. They probably did, in many cases, provide the money directly to—

Mr. Frank Baylis: They didn't even trust them to give them the money. They just said, "Send the invoice to them and we'll pay it."

Mr. Christopher Wylie: I'm sorry. I stand corrected. The invoices were different, but the money did—

Mr. Frank Baylis: They didn't even bother sending the money. That's how coordinated they were.

Starting off right at the beginning of this issue, I'd like to talk to LUKOIL and the Russian government. LUKOIL, as we know, is run by a gentleman, Mr. Alekperov, who is a former minister of the government. We know that this company is under U.S. government sanctions because it's seen as an arm of the Russian government, so when I talk about LUKOIL or I talk about the Russian regime of Vladimir Putin, I'm going to be referring to them as one.

They start off by connecting with Mr. Kogan. Can you explain those connections between Mr. Kogan and the Russian government?

Mr. Christopher Wylie: At the time Dr. Kogan was engaged by SCL, he was also working on Russian-funded projects out of St. Petersburg on profiling social media users, with a particular focus on two things. One was online trolling, and trolling behaviour in all social media. The second was a focus on what you call "dark triad traits," which are narcissism, psychopathy, and Machiavellianism.

SCL was aware of this work. It is documented in emails that the company wanted to pitch Aleksandr Kogan's work for the Russians to its other clients. They were giving talks, as I understand it, both about the work he was doing at St. Petersburg and also referencing some of he work he was doing for SCL in the United States.

Around the same time, LUKOIL then approached SCL/Cambridge Analytica with a particular interest in targeting. Discussions were had about Cambridge Analytica's experience in rumour campaigns and disinformation. That is documented. There were presentations, which I've handed out to the authorities, that reference back—

● (0920)

Mr. Frank Baylis: I want to hold that thought for a second. So LUKOIL, again, this theoretical oil company, shows up at SCL, and they want to talk about rumour campaigns, attitudinal inoculation, things that we could call "fake news". Would that be a global catch-all?

Mr. Christopher Wylie: Sure. That's sort of a new way of calling it.

Mr. Frank Baylis: Yes.

Mr. Christopher Wylie: It's disinformation.

Mr. Frank Baylis: Let's call it fake news. That seems to be the term now.

Mr. Christopher Wylie: Sure.

Mr. Frank Baylis: Why would LUKOIL be interested in fake news or spreading fake news?

Mr. Christopher Wylie: I can't speak to what LUKOIL's intentions were in terms of those meetings. I do know that when SCL made presentations about disinformation or attitudinal inoculation, that did not dissuade the company from continuing that relationship. The company was interested. They then received white papers that my colleagues and I had composed on the data assets and capacity of the company in the United States.

Mr. Frank Baylis: If I could say at this time, at this stage, you've got LUKOIL—which I'm going to call the Russian government—trying to spread fake news and learning about.... I need a database so I'm working with Mr. Kogan to get a database and I'm financing him, the Russian government, LUKOIL. Then I'm also talking to SCL about how to spread that fake news now that I have this database. That's going on.

Then something interesting happens. Two people from the United States show up, Mr. Steve Bannon and Robert Mercer. The big players in the Internet are all American-based. This technology to target people...as you mentioned, Canadians can do it, Americans can do it. How did Steve Bannon and Robert Mercer know that this was going on, that there was this group working with the Russian government that was stealing data, and then looking at spreading fake news? How did those two gentlemen show up—Steve Bannon and Robert Mercer—to this little company in Cambridge?

Mr. Christopher Wylie: I wasn't present for the first couple of meetings. My understanding is that Steve Bannon was introduced to Alexander Nix by a mutual acquaintance. At the time he was the editor of Breitbart and was a follower of what's called the Breitbart doctrine, which is that politics flow downstream from culture, so if you want to change politics, start with culture. Breitbart, obviously, was not expanding into a mainstream media outlet as had been envisioned. He was looking for a way of expanding his arsenal of tools to engage in what he would call culture war. So the appeal of SCL Group, when he was introduced to the company, was that it worked on information operations for the U.S. military, for the U.K. military, and for other militaries.

Mr. Frank Baylis: Could we say another appeal might be that they happen to have something unique, something that wasn't available in this space? Could we say that one of the appeals was that they had a Russian who had stolen a lot of data that they could put to work? Could we say that that might have been a unique aspect that brought them there?

Mr. Christopher Wylie: I just want to make a small correction on the timelines. The Kogan project began after Steve Bannon took over the company, but it was authorized by Steve Bannon. So in terms of the timeline, the work that Aleksandr Kogan engaged in happened after Steve Bannon and Robert Mercer had acquired the IP in SCL, set up Cambridge Analytica and then deposited the funds to pay for it.

● (0925)

Mr. Frank Baylis: The work, the actual scraping of the data, is that what you mean?

Mr. Christopher Wylie: Yes, so that means—

Mr. Frank Baylis: That means that they knew that he was working with the Russians. They show up there and they know he has a special skill set to scrape data. Is it possible the Russians let them know about it? Did you ever see a link between Mr. Bannon, Mr. Mercer, and LUKOIL directly, or is there any hint of that?

Mr. Christopher Wylie: Well, Steve Bannon had to approve all of the projects that the company engaged in. As the vice-president, he was in charge of managing the operations on a day-to-day basis, albeit in the United States. Any new clients or new projects or new stream of work, particularly if it incurred a cost, would have to be approved by him. He was aware—

The Chair: Thank you, Mr. Baylis.

Mr. Frank Baylis: Go ahead and finish up.

The Chair: Go ahead and finish your answer.

Mr. Christopher Wylie: He was aware of the work that was going on. He was aware of Dr. Kogan's work, and he approved the financing of it. To highlight the scale of it, the company spent close to $1 million in the first three months of that project, so that had to be approved by Steve Bannon and the Mercers.

The Chair: Thank you, Mr. Wylie.

Next up for five minutes is Monsieur Gourde.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair.

Mr. Wylie, when you designed the architecture for the technology, did you start with a blank slate, or did you model it on some other piece of technology that existed in the world?

[*English*]

Mr. Christopher Wylie: When I first got engaged by the SCL Group in the summer of 2013, they were looking at modernizing a lot of their activities and work, particularly as they related to what was happening in the defence community, which was an expansion of research into the proliferation of ideas online and social media, because that was fast becoming one of the primary recruitment tools of extremist organizations and terrorist organizations. The company had a deficit in technical expertise, and it wanted to expand that, so when I came on board, it was in part to look at the operations of the company and figure out how it could modernize its tactics and use technology to improve that.

When I started, you could call it a blank slate in the sense that the technological infrastructure was not yet there. It was not a blank slate in the sense that the company had several decades of experience working in information operations around the world, so part of the role, at least initially when I was invited to join the company, was to look at existing tactics and techniques in information operations and see how we could import that into cyberspace.

[*Translation*]

Mr. Jacques Gourde: Mr. Wylie, how does a piece of military technology transform into a tool for election campaigns in a democratic jurisdiction? Did you receive orders from third parties? You didn't do it simply for fun. You no doubt saw the market potential, in terms of people willing to pay for this kind of technology.

[*English*]

Mr. Christopher Wylie: To be clear, when I was first engaged by SCL, I became research director for multiple companies, so it wasn't just the elections division that I was working on. Looking at the research we were doing originally, it wasn't necessarily just for elections. There would have been military applications for it, and at the time, military work was the bread and butter of the company. It was around that time that Alexander Nix met up with Steve Bannon and began that process of engaging with Bannon and the Mercers to essentially port that over into an electoral context in the United States.

● (0930)

[*Translation*]

Mr. Jacques Gourde: Did political parties contact your company looking for the help your technology could provide, or, conversely, did your company reach out to political parties to let them know it had something that could help them seek out potential voters?

[*English*]

Mr. Christopher Wylie: Alexander Nix usually handled the relationships with clients, or perspective clients. I do know that he went out and met with several prospective clients mostly in Africa or the Caribbean, some in South America and in Asia, about some of the work that was being done. I wasn't necessarily present in those meetings, so I can't speak to that.

[*Translation*]

Mr. Jacques Gourde: You're confirming, then, that your company specialized in reaching out to people in different countries to help them with election campaigns. Your technology was specifically developed for a global market of democratic influence, was it not?

[*English*]

Mr. Christopher Wylie: Yes. Part of the work that the company did was to go into other countries and work in election campaigns, particularly in emerging democracies. The way that the company often made money was not necessarily from working in elections, but rather using the relationships that it built in those campaigns later for government projects.

The Chair: Thank you.

Next up, we have Ms. Vandenbeld.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you for being here to answer our questions.

I'd like to go to something you told the U.S. Senate judiciary committee, about where you really drew the line. You said that one of the things that caused you to blow the whistle on this was because they were starting to engage in voter suppression, particularly targeting people based on their race. Could you explain what it is exactly? When you're talking about voter suppression, what is it they were proposing or did do?

Mr. Christopher Wylie: To be clear, I didn't work on voter suppression projects. I was made aware of them while I was there.

My understanding of what the company was intending to do—I believe at the instigation of Steve Bannon and some of his colleagues in different packs—was to create lists of predominantly African American voters and then look at what types of messaging would disengage them from politics further, which would then reduce the likelihood that they would vote.

There are different definitions of voter suppression. The most egregious form would be to actually go and try to deregister people from voting, by what's called vote caging. That's not what I'm talking about. What I am talking about is finding things that will make politics so unappetizing or confusing to a subset of voters that they become less inclined to actually vote or engage with the democratic process.

Ms. Anita Vandenbeld: This is based on these psychosocial behavioural profiles that are gathered from, as you mentioned, not just Facebook, but potentially private companies and different sources, like browsing histories and things like that. Is there this aggregate of data that is being collected that is allowing this kind of this work?

Mr. Christopher Wylie: Yes. The data would be sourced from multiple origins. Some of it was commercial, some of it was electoral, and some of it was social or online.

Ms. Anita Vandenbeld: One of the things you told us was that the intellectual property of AggregateIQ, a lot of this data that's being collected and aggregated, is actually exclusively owned by SCL. There's a data-sharing arrangement. When Mr. Vickery was testifying before the committee, he said a similar thing. He said that he found on the servers of AIQ data where the code base looked like it was exactly the same, which again suggests that SCL and AggregateIQ were sharing their data completely. However, when we had Mr. Silvester here, he said that all they had access to was potentially some ranking scores that came from the U.S. that might have come from an SCL server somewhere.

You're saying that what Mr. Silvester told us is not accurate, but that in fact, there was a much closer arrangement between SCL and AIQ.

● (0935)

Mr. Christopher Wylie: In order for the technologies AIQ was developing to work, what they built was the interface between databases and online platforms that you could put advertising on. They were that sort of middle ground. You need to have access to the data in order to pull lists, in order to send it and to create a custom audience.

You can't build a targeting platform that doesn't have access to data, because then what are you targeting on, right? One of the things I provided to the DCMS committee here in Britain is an email from AIQ that specifically references searching the SCL databases on the Ripon project.

I don't know how else you can query a database if you don't have access to the database. I do not know how you can perform targeting if you don't have access to the database. Frankly, I'm surprised and really disappointed that Jeff Silvester and Zack Massingham have decided to try to obfuscate or hide what happened. You'll have to ask them why it is that they are taking this line, but in my view, that's just not true. What value would they offer, then, if they did not use any of the data?

Ms. Anita Vandenbeld: That's my next question. When people are engaging SCL, Cambridge Analytica, or AggregateIQ, particularly for elections, what are they buying?

What we were led to believe through AggregateIQ is that it's like Burma-Shave: you just put a little thing on Facebook, and they were just the ones that put on the ads, based on some demographic data on Facebook. If somebody waves at you on the street, it's the same thing as putting on a light; they were just gathering that, and that was all they were doing, but 600,000 pounds for a single contract just so someone can go and target some people on Facebook, which most people or any volunteer could probably do...?

You're suggesting that what they were really buying was access to this aggregated database, this psychosocial profiling, this vast amount of data that was collected. That's what people were buying into.

Mr. Christopher Wylie: I appreciate your very Canadian political term of "Burma-Shave". I haven't heard that in a long time.

Voices: Oh, oh!

Mr. Christopher Wylie: The thing that I find farcical is the line that all AggregateIQ does is just click some demographic on Facebook Ads Manager and that's it. The problem I have with that is, I'm like, well, what is the value of your company then? All you're doing is something an intern could do, right?

If you know that you want to target women between 25 and 30, you can tell your intern to go and do that. I don't understand why you would need.... It would be a lot cheaper, also, because you wouldn't have to be paying for all the consultancy fees. To me, that's just farcical as an explanation, unless they are grossly incompetent or.... I don't know if Vote Leave was just that stupid, but having met Dom Cummings, I don't think he is, so I find that really hard to believe.

One of the things that Facebook has gone out and confirmed is that a lot of these different campaigns were using the same custom audiences for targeting. I don't understand that explanation, and I can't speak for them, but for me, I don't buy it.

The Chair: Thank you.

Next up for five minutes is Mr. Kent.

Hon. Peter Kent: Thank you very much.

Mr. Wylie, you mentioned the technical briefing that you gave to Mr. Cummings and the Brexit Leave campaign. Certainly, all Canadian political parties collect data, but we don't collect the sort of deep data that would allow what you describe: "With a deep understanding of underlying cognitive and dispositional processes, we can get to the heart of why people are driven towards almost any behaviour...".

You talk about "personality psychometrics"—about vulnerabilities, really—of individual voters, who you say sometimes lie to themselves about what they want to do or the choices they want to make, but I think the most telling line is at the end of your briefing, where you say, "This is because we can trigger the underlying dispositional motivators that drive each psychographic audience."

Again, you claim at the beginning of this technical briefing that you would engage your "multinational team that combines years of experience in micro-targeting and psychographic profiling in British, American, Canadian and international politics". This comes back again to The Canadian Press, a reliable source of news in Canada, which reported earlier this year that an acquaintance of yours, off the record, not identified—

● (0940)

Mr. Christopher Wylie: It's hard for me to comment on somebody who claims to know me or what happens, if I don't have their name, if I don't know why they said that.

Hon. Peter Kent: This acquaintance said that they had drinks with you—

Mr. Christopher Wylie: Let's be clear. I don't know if they're an acquaintance or not.

Hon. Peter Kent: Let me describe the situation and you may recall. This acquaintance said he or she had drinks with you in Ottawa in November 2015, a few weeks after the federal election, and the same acquaintance was quoted by Canadian Press as saying you were shopping your Facebook data-mining techniques in Ottawa with the Liberals and in Washington with the Republican Party and that you discussed with this acquaintance—

Mr. Christopher Wylie: That's not—

Hon. Peter Kent: —your ethical concerns. Is that inaccurate?

Mr. Christopher Wylie: Let me be clear. That is not accurate. Let me be just super-clear right now. That is not accurate. I was not in the United States at that time pitching the Republican Party. I welcome you to ask the RNC if I was there doing that. It's just not true.

In terms of Facebook, I don't even know where to begin with this. When you are looking at underlying motivators of people, for example, that does not mean you have to do anything nefarious. For example, if people are more extroverted, they like things that have a higher audiovisual content in them, so you might want to send them something that is more flashy or more fun, compared to people who are more introverted who might want to read something more in-depth. They're conscientious, for example.

I would just caution people about twisting anything to do with data or anything to do with the underlying psychology of voters into something nefarious when it doesn't necessarily have to be.

To be clear, I didn't work for the Liberal Party. I haven't worked for the Liberal Party in I don't know how many years, but a long time, since before I moved to the U.K. The work I did for the LRB was simply helping them when they were transitioning—because this was the time that the government was just being set up—on looking at caucus communications, looking at basic metrics on things like Twitter, what people are talking about. There was nothing nefarious about that. To be clear, I haven't worked for the Liberal Party or any Canadian Liberal entity on psychographic targeting. Let me just be super-clear. Any insinuation that I have done that is just untrue. I have not worked on psychometric-based targeting for the Liberal Party or any Liberal entity.

Hon. Peter Kent: Even though you told Mr. Cummings that you did? You said—

Mr. Christopher Wylie: No, the reference—

Hon. Peter Kent: —in this email from you—

Mr. Christopher Wylie: The reference you're making is to discussions that I was having about what could be done. My role—

Hon. Peter Kent: Just to be clear, you referred specifically to the in-depth technical briefing on psychographic micro-targeting and you also said, "Some of us will be in Ottawa this month working on a similar project for a major Canadian political party". Were you misleading Mr. Cummings?

● (0945)

Mr. Christopher Wylie: No, let me be clear. I did not work on a project related to psychographic targeting for the Liberal Party—

Hon. Peter Kent: Let's move on, then.

Mr. Christopher Wylie: —and that's the end of it.

Hon. Peter Kent: We'll continue a little bit later. Thank you.

The Chair: Next up for five minutes is Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon, I guess, to you, Mr. Wylie.

I have just a quick question. This is something regarding the testimony you gave last week and it was with Senator Whitehouse. It's an exchange you had with him. In response to a question from Senator Whitehouse last week about AIQ and SCL Group Canada, you stated, "There are subcontractors that were set up during the time that I was there to build out software infrastructure." As I'm sure you know, they completely deny being set up in order to serve SCL or Cambridge Analytica.

Can you go through the process or give us an idea of what was undertaken to set them up, in as much detail as you can?

Mr. Christopher Wylie: My understanding is that AggregateIQ as a company was only very recently set up before the first contract it engaged in. That's something that could be checked, actually—when the company was actually set up—because before that point, Jeff Silvester and Zack Massingham were working in other companies. They left to form this company so they could then work on SCL-related projects. That perhaps is a question better placed to AggregateIQ, as they would have the company documents for that.

They started working under the auspices of AggregateIQ once they were offered substantial projects in the Caribbean, in Africa, and then later in the United States. The contractual arrangement that was made was that the intellectual property that they would be developing, which SCL was paying for, would be owned by SCL.

Mr. Raj Saini: Just to touch on that point, AIQ was set up because you had an initial conversation with them about potential work. Prior to that, there was no AIQ. There were just two guys and they had no....

Mr. Christopher Wylie: Yes, that's my understanding.

Mr. Raj Saini: So AIQ was set up because you had that initial conversation with them and you said there was some work that you would like them to do, and you had the discussion about their coming to England. But as you stated, they had families and they had recently purchased a home so they would have preferred to work with your company solely, but to do it in Canada.

Mr. Christopher Wylie: Yes.

Mr. Raj Saini: The next question is one that was in front of the U. K. committee. You noted that, and I quote, "If you can bill as several different companies but it is the same team working on it, the paperwork looks compliant even if the project is not."

To your knowledge, were there any discussions between SCL and/or Cambridge Analytica with AIQ regarding the intentional flouting or circumvention of domestic laws or any sort of expenditure-related rules, and if so, what was the nature of those discussions?

Mr. Christopher Wylie: What I can say is that work was performed in the United States by AggregateIQ, by SCL, and by Cambridge Analytica, and oftentimes those were for various PAC's or campaigns or other electoral entities that were working in the same state, same region, or same electoral context. As to the specific discussions that AIQ has had with SCL, you'll have to ask AIQ.

One of my concerns was that the set-up of this arrangement would allow the various entities collectively to perform work that they otherwise would not be allowed to, had the regulator known that it was the same people just wearing different hats. The company SCL and Cambridge Analytica actually received legal advice on this and on other matters related to compliance in the United States. I'm not confident that they followed through with that advice.

AIQ's work in the United States potentially is questionable if they were, for example, sending non-American citizens down to advise or manage a campaign contrary to ethics rules and American law.

● (0950)

Mr. Raj Saini: I have several other questions but I'm going to ask you a shorter question. Also, and this is from your testimony last week with Senator Whitehouse, you noted that the Ripon tool was created in order to use the data harvested by Aleksandr Kogan. Do you find it credible that AIQ wouldn't have been aware of the fact they were building this tool and for what purpose?

Mr. Christopher Wylie: They were fully aware. They came to the U.K. all the time. I think they might have even met Aleksandr Kogan. I'm not sure exactly if they had or not. But I recall their being there when Aleksandr Kogan was in the office, also. I find it—

Mr. Raj Saini: They would have been aware.

Sorry, go ahead.

Mr. Christopher Wylie: I find it really difficult to believe that they went through an extensive contacting process, an extensive technical specification and did not understand the specification that they were co-writing.

Mr. Raj Saini: Thank you.

The Chair: Next up for three minutes, Mr. Angus.

Mr. Charlie Angus: Thank you, Mr. Wylie.

I want to ask you about a conversation you claimed to have had with Jeff Silvester that he remembers differently, and you did swear under oath. I just want to make sure that what you said was accurate because you had stated in other testimony that, and I quote:

> They [AIQ, Jeff Silvester] conceded to me, and this is a verbatim quote—and I stand by it; I remember Jeff Sylvester telling me...[that what they did] was "totally illegal". [...] ...that AggregateIQ was just used as a...money-laundering vehicle.

Is that true? Did that conversation happen?

Mr. Christopher Wylie: Yes. It happened in the spring of last year in Victoria, British Columbia. The words "totally illegal" I distinctly remember.

I stand by my recollection of that.

Mr. Charlie Angus: We asked Mr. Silvester about it. He said he was very surprised that you said that he said it was a misunderstanding, and that he wrote a text to you expressing that he thought it was a misunderstanding. Would that be true?

Mr. Christopher Wylie: No, that's not true. I have all of the text messages from Jeff Silvester at that time. I absolutely do not recall his correcting his statement via text message.

Mr. Charlie Angus: Would you share—

Mr. Christopher Wylie: I don't believe that for a minute.

Mr. Charlie Angus: Would you share those text messages with our committee? We're not interested in whether you talked about the Blue Jays or Liverpool, but whether or not he was concerned that he had been misrepresented to us is very important.

Mr. Christopher Wylie: Sure, absolutely.

What I'll do is speak to my lawyers, and we'll find the best way to provide you with the information that you would like.

Mr. Charlie Angus: Thank you very much.

Again, I'm concerned about the role of AIQ in various other roles with Cambridge Analytica. We asked about the murder video in Nigeria, and to AIQ's credit, it seemed that it was very upset when it received the murder video. Who gave AIQ the murder video?

Mr. Christopher Wylie: The video that you're referring to is a video that shows people being dismembered. It has highly Islamophobic messaging in it. Cambridge Analytica—I believe actually via a contractor—created that video, and then sent it to AIQ for distribution. So, AIQ did not create the video. However, it—

Mr. Charlie Angus: No, and to AIQ's credit, it seemed very upset by that video. What surprised me was that Zack Massingham said at our committee that he didn't know that Cambridge Analytica existed during the Nigeria campaign, so he didn't understand how.... This made me wonder about who gave AIQ the video, if it came from Cambridge Analytica? How did he not know—

Mr. Christopher Wylie: That cannot possibly be true. I'm sorry. That just can't be true. To not know who your largest client is.... I'm surprised that he said that.

Mr. Charlie Angus: He has a phone that he didn't know he had.

Voices: Oh, oh!

Mr. Charlie Angus: I just want to get this on the record.

So, you're saying that it's absurd that in the Nigeria campaign, this video originated with Cambridge Analytica. It was handed to AIQ, but AIQ said that it didn't know that Cambridge Analytica existed.

Mr. Christopher Wylie: Unless they're.... I don't know. Frankly, I'm shocked that he said that because it was the largest client of AIQ. I don't know how the CEO of a company doesn't know who its largest client is.

Mr. Charlie Angus: I'm just going to close this off because we have to go on. I'm worried about Mr. Massingham. Is he taking the fall for somebody? Why would someone totally misrepresent a simple fact like that?

● (0955)

Mr. Christopher Wylie: Honestly, I'm actually speechless that he said that. I honestly have no idea how to explain that. I think it's unfortunate because there's a lot of information that I think is really important for people, regulators, and legislatures to know about. They had every opportunity to participate in blowing the whistle, and they decided not to, so you'll have to ask him that. I find it absolutely shocking that he didn't know what Cambridge Analytica was, when it was AIQ's largest client.

Mr. Charlie Angus: Thank you.

The Chair: Just so everybody knows, we're going to go into the next round right away.

There's possibly a time allocation vote that's going to happen within about 20 minutes, so just hang in there, Mr. Wylie. We're going to keep going as much as we can.

I don't know if you're okay. Do you need a health break or anything like that, Mr. Wylie?

Mr. Christopher Wylie: I'm okay.

The Chair: You're good to go.

Okay, we'll continue as scheduled with Mr. Picard for seven minutes.

[*Translation*]

Mr. Michel Picard (Montarville, Lib.): Thank you.

Mr. Wylie, I'm going to pick up on a few points of interest from your remarks.

Why were these companies incorporated in Canada? Given the international clientele and the scope of the work, were AIQ and SCL incorporated in Canada for practical or regulatory reasons?

[*English*]

Mr. Christopher Wylie: It was simply because that's where Jeff Silvester and Zack Massingham lived and wanted to stay. They wanted to participate in SCL projects, but they had the temporal and geographic constraint of being in Canada rather than moving to the U.K., so the company accommodated that.

[*Translation*]

Mr. Michel Picard: Now I'd like to turn to the data you collected or, rather, the data you worked on.

I'm going to draw an analogy. In cooking, you can be as creative as you want in coming up with all kinds of dishes. The real problem, however, is where the ingredients come from.

In this case, the detail we are missing is the source of the data you used for your analyses. Strictly speaking, when you work on something that is given to you, you do the job you're being paid for. I'd like to know whether you were responsible for acquiring the data or whether it was the responsibility of the people or companies you worked for?

[*English*]

Mr. Christopher Wylie: Sorry, when you refer to the source of the information, are you referring to the Kogan project? Is that what you're referring to?

[*Translation*]

Mr. Michel Picard: You can provide a more general answer. The Kogan issue is rather specific.

When you want information from a variety of databases, you have to get it. It isn't simply available; you have to acquire it, so you need an agreement with the data provider.

The issue is multi-faceted. Does the owner of the data initiate the transmission of the data? Facebook, for instance, has datasets. Does it give you access to those data, either loaning or giving them to you? Does someone buy the data? Are the data obtained by hacking?

[*English*]

Mr. Christopher Wylie: This is not intended to be a difficult answer. It's just that it depends, really, on the project and the data source that you're talking about.

For example, the Facebook dataset was acquired by Aleksandr Kogan using apps from Facebook. Other datasets were acquired, some at the instigation of the owners of those datasets. For example, clients would sometimes provide the company with information, so they would help that modelling process.

In other cases there would be a contractual relationship directly with a company—a data vendor that sells consumer data, for example, or a company that sells its customer lists.

In other cases, subcontractors would be used to go and acquire data generally, depending on what they would go and find. For example, AggregateIQ was sometimes tasked with finding datasets for particular projects. They did that in Trinidad, for example. They went out and acquired data on behalf of the company.

Sometimes it's a contractual relationship directly with the data vendor. Sometimes it's an application that collects data. There are a lot of different ways you can collect data.

● (1000)

[*Translation*]

Mr. Michel Picard: In the case of Brexit, you seemed surprised by the fact that you were working on information that was relatively the same, regardless of the party in question.

Normally, it is someone looking to obtain power or hoping to control the group that will be in power who is interested in manipulating information for political gain or even manipulating a democratic process like an election. In the case of Brexit, I saw that there were contracts with people in the Caribbean, Africa, and the U.S., but it could apply in other cases as well.

Are you aware of foreign interests that would like to use this kind of technology to get their hands on power in certain countries?

[*English*]

Mr. Christopher Wylie: I'm aware of projects for which clients from one country would be interested in electoral results in another. To my understanding, SCL did participate in projects for which some of the funders would not be nationals or residents of the country that they were operating in.

For example, you have companies that might be interested in the natural resources of a particular country, and one government versus another may be more conducive to that.

I am aware of the company generally engaging with nationals of other countries for a project in a separate country.

[*Translation*]

Mr. Michel Picard: Earlier, you distinguished between voter suppression and vote caging, which consists in removing people's names from the voter list.

To your knowledge, did AIQ, SCL, or other entities engage in the practice of taking people's names off the voter list?

[*English*]

Mr. Christopher Wylie: I'll be super-clear. When I'm talking about voter suppression, I'm not speaking about vote caging, or literally removing people from the electoral register. What I'm talking about is targeting particular groups of people with messages that will disengage, frustrate, or confuse them. That ultimately will, in some cases, inhibit or demotivate them enough to not participate in an election.

[*Translation*]

Mr. Michel Picard: What I was asking was whether you took part in vote caging.

[*English*]

Mr. Christopher Wylie: No.

Mr. Michel Picard: Thank you.

Thank you, Chair.

The Chair: Thank you, Monsieur Picard.

Next up for seven minutes is Mr. Kent.

Hon. Peter Kent: Thank you, Chair.

Mr. Wylie, in coming back to your associations with the Liberal Party of Canada, Braeden Caley, a Liberal Party spokesman, told Canadian Press in an email that the party did not contract you to do any work after staffers met with you in January 2016. A spokesperson for Prime Minister Trudeau, Chantal Gagnon, told CP in a separate email note, "Mr. Wylie did some preliminary work for the Liberal caucus research bureau, but ultimately it was decided not to move forward with his services". What services were you paid for, for the $100,000 you received in January 2016? Were those services rendered before the 2015 election or in 2016?

Mr. Christopher Wylie: First of all, I haven't worked for the Liberal Party of Canada, the political party.

Hon. Peter Kent: I understand; it was the research bureau.

Mr. Christopher Wylie: The research bureau at the time was looking for ways to optimize caucus communications, of responding better to constituents, constituent communications, and also providing the caucus with ongoing information as to, for example, what people are speaking about on Twitter. A lot of the work that I did in relation to the LRB was—and the word "preliminary" is appropriate because it was a new government at the time. They were just setting up the office, so they wanted help with whom they should be hiring; what they should be doing; how they should be collecting insight to inform caucus meetings when they're talking about issue x or issue y; and more broadly, how to optimize communications with constituents, for example, managing correspondence and things like that.

A lot of that was to help them, as they were setting up, as they were transitioning into government, and as they were hiring their staff. I didn't want to become a staff member. It wasn't necessarily something that I envisioned doing for a long time. The work that was done wasn't necessarily groundbreaking or anything. It was just to help the LRB during that transitioning process.

● (1005)

Hon. Peter Kent: Do you think the Liberal research bureau is working on its own, without your continuing services, to develop psychographic micro-targeting in the next election?

Mr. Christopher Wylie: Again, to be clear, the work that was being done did not involve micro-targeting. The role of the LRB is not an election entity; it's to support the work of the caucus. The focus of the LRB is to look at policy issues to find out things like what people are talking about. If their next meeting is going to focus on northern affairs, they want to know what people talking about, what they think. That way you could have a more informed caucus discussion. You can do that either by hiring a lot of interns to go through and pull out examples of tweets and things that people care about, or you can do it programmatically, or you can hire somebody to build it programmatically.

Hon. Peter Kent: To achieve what you said, "trigger the underlying dispositional motivators that drive each psychographic audience", you need much more than a name, an address, a phone number, and an email. You need what you go into, in quite specific depth, additional information on personality, on personality vulnerabilities and so forth to be able to, as you say, drive a voter to where they may not know they want to go. Is that not correct? Isn't that what—

Mr. Christopher Wylie: I wouldn't necessarily agree with your characterization of it. It is very well known in behavioural research that people often do not have insight into some of their own behaviours: for example, if you ask people how much they smoke, how much they drink, how many vegetables they eat, you'd typically get responses that do not reflect the actual behaviour. Depending on the context of the work you're doing, sometimes it's important to find other indicators that are more reflective of the behaviours you're interested in.

For example, in voting a lot of times people will say they're unsure as to how they're going to vote. That doesn't mean they won't have a consistent voting behaviour; it just means that at the time they haven't thought about it and they're not necessarily going to give you a helpful answer. If you can find other indicators of that, that's all that means. There's nothing nefarious about it.

I can guarantee that every party in Canada does modelling projects that look for indicators in voting behaviour.

Hon. Peter Kent: But they don't—

Mr. Christopher Wylie: The Liberal Party does that; the Conservative Party does that; the NDP does that.

Hon. Peter Kent: They don't gather data of the sort improperly harvested from Facebook, which show prejudices, biases, vulnerabilities, which were, obviously, used by AIQ in the Vote Leave campaign, the Brexit campaign, and reportedly in American elections.

Mr. Christopher Wylie: Sure.

Hon. Peter Kent: The question is, if the data that's acquired is beyond the name, the email, the phone number, the basic voter ID that all parties, you're quite right, do, which we use to get out the vote.... I don't go looking, and certainly I don't believe my party goes looking, for the vulnerabilities of the voters in my constituency to try to change their opinion or to try to change their voting intention because of the vulnerabilities that may be indicated by improper harvesting of data elsewhere.

Mr. Christopher Wylie: Sure. Nor does the LRB and nor does the Liberal Party, at least at the time that I was there.

Hon. Peter Kent: It seems that contrary to your statement that it's uncomfortable to consider our democracy may have been corrupted, you don't believe that psychographic micro-targeting corrupts our democratic electoral process?

● (1010)

Mr. Christopher Wylie: It's if used properly. Again, this is why I keep stressing that just because data or psychology is involved does not mean that innately there is something nefarious is going on. There is a problem around the world, in Canada also, with voter disengagement. Fewer and fewer people turn out to vote. This is because there's a new media environment that is distracting and people are disconnected with politics, and oftentimes it is very helpful to understand, again, underlying motivators for people so that you can improve turnout, you can improve voter engagement, and you can speak to people in a way that motivates them and wants them to participate. That is a use case that is not nefarious; it is a positive use case because you are looking to increase turnout and increase participation in your democracy. Just because data is used or just because psychology is used does not mean that you are going to seek out misappropriated data; it does not mean that you are out to manipulate or coerce or somehow trick or suppress voters. It just means that you are looking for information to help you engage those people.

Hon. Peter Kent: Certainly your technical briefing would seem to be, if not nefarious, suggesting unethical manipulation of voter intention.

Mr. Christopher Wylie: I disagree, and that briefing was sent to the Information Commissioner's office and The Electoral Commission. I proactively gave it to them and there is nothing in there that is illegal or goes outside the boundaries of the law.

Hon. Peter Kent: It's a fine line.

The Chair: Thank you.

Next up, for seven minutes, is Mr. Angus.

Mr. Charlie Angus: Mr. Wylie, I'm very interested in your analysis of the role of SCL that worked with Cambridge Analytica and AggregateIQ on some of these international projects that, I believe, you referred to as a form of new neo-colonialism. Would you say that that's the correct term that you used or did I get that wrong?

Mr. Christopher Wylie: I've had several conversations now with representatives of governments in different countries. One of the things that has become very apparent is that you might have a country that gained independence and the former colonizer left, but corporate interests didn't. What I mean by neo-colonialism is, rather than state action or government action to control via a governor the affairs of a particular country, you have large multinational companies or wealthy individuals from, oftentimes, the former colonizer coming in and seeking to interfere with the elections in a way such that resources, for example, can continue to be extracted in a way that is conducive for business interests in that former colonizer. What I meant by that is that colonialism still happens in a lot of these places, it just doesn't look like the form that it did 100 years ago.

Mr. Charlie Angus: Right. I think this is fascinating because I'm looking at the work of SCL, Cambridge Analytica, AIQ in Nigeria, Trinidad and elsewhere, and it's like some kind of Frederick Forsyth novel with cyber-geeks.

I just want to go through a bit of this. In the Nigeria campaign, there was the question of the murder video that was to incite ethnic hatred that was brought forward by a Cambridge Analytica operator that was supposedly given to AIQ. In Trinidad and Tobago there are allegations that illegal data was collected and harvested; there was the deanonymizing of emails—is that correct?—and AIQ was involved with that?

Mr. Christopher Wylie: It was clickstream data of Internet browsing history.

Mr. Charlie Angus: AIQ worked with Cambridge Analytica for SCL on those projects?

Mr. Christopher Wylie: Yes.

Mr. Charlie Angus: You had stated that this is a company that has gone around the world and undermined democratic elections in all kinds of countries and that they could care less as to whether their work is compliant, because they like to win. Is that correct—on SCL and the culture that came out of Cambridge Analytica and AggregateIQ?

Mr. Christopher Wylie: That was the impression I got when I was there.

Mr. Charlie Angus: The Canadian government paid SCL to run psychological operations in Latvia, and said that—

● (1015)

Mr. Christopher Wylie: At the NATO StratCom centre.

Mr. Charlie Angus: It was promoted by Canadian Ambassador Alain Hauser and the Latvian secretary of defence that they would use the SCL team of experts in target audience analysis. Would that be similar to what they could have done in Brexit, this target audience analysis? Can you explain that?

Mr. Christopher Wylie: Target audience analysis, or TAA, is the starting point for information operations in a military context. It's something SCL specialized in. If you take a step back for a moment and look at information operations as a military endeavour, it's part of what's called multi-dimensional battle space, where you as the military client are trying to seek out dominance in all of those spaces, whether it's land, sea, airspace, or indeed, information. TAA is the starting point where you look for the information space around your target and identify weaknesses or vulnerabilities in that information space, whether to deny your opponent information or to provide them with information that is conducive to your operational objective.

Mr. Charlie Angus: Part of the tail of this big dog that we've grabbed is the illegal end, so we just see these guys as dodgy operators who are out to do dodgy things, yet they get hired by NATO to do dodgy things on behalf of the Canadian people. Now they've morphed into Emerdata, which seems to be all the same players, but they also include financial links to Blackwater, the mercenary group, and they've worked with Black Cube, Israeli black operators.

How are we to navigate a space where a large corporate interest can do completely illegal things in one context and then be brought in by governments to do favours for them in others?

Mr. Christopher Wylie: Information operations are not always nefarious or a bad thing. If you think of a conflict—

Mr. Charlie Angus: You said that this is a company that's gone around the world and undermined democratic elections, and they don't care whether their work is compliant, because they like to win. This is a corporate culture we're dealing with.

Mr. Christopher Wylie: Yes. Sorry, it was a broader point on, for example, projects that Canada funds. Just because Canada funds an IO project does not mean that Canada is intending to undermine democracy around the world.

When you look at counter-extremism, if you seek to confuse or interfere with the operations or communications of an extremist group or a terrorist group, that is ultimately a denial of their agency. But in that context, it may be appropriate.

Mr. Charlie Angus: I get that.

The question for me is legislation. If we have companies that engage in nefarious, illegal activities, but we can say that the enemy of my enemy is now my friend, how do we legislate companies that seem to be so willing to break the law, but then still get government contracts because it's useful to have them do work elsewhere?

This is something we need to be talking about, but we haven't really dealt with it. I'm asking your opinion from having worked inside with them.

Mr. Christopher Wylie: When you take a step back, Canadians often—and rightly so—think of Canada as a country that goes around the world and promotes democracy. In doing so, you are strengthening civic institutions, and you are helping people participate.

When you look at the actions of Canadian companies, for example AIQ, they are doing the exact opposite of that. Canada as a country does not know about that activity because it does not require, for example, proactive registration of any kind of activity in a foreign election.

One of the things that I've been speaking to American members of Congress about is that in the same way that you have to register foreign agents who are lobbying or conducting work in the United States, you should also have a registry of companies that are doing work outside in other elections or in electoral contacts to allow oversight, whether that is government oversight or civic society oversight of the operations of companies in other elections.

I don't know if the Canadian government was aware that SCL also had an elections division. One of the things that could be done is better due diligence about what the other projects and activities are that the company being contracted by the Canadian government is doing in other places.

The question is simply, what other projects have you done in the past two years or are you currently working on and are any of those political?

● (1020)

The Chair: Thank you.

Next up for seven minutes is Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: Thanks very much.

It's great that we've been working in a non-partisan way, although today Mr. Kent seems to be more partisan than usual. I look forward to him inviting Hamish Marshall to our committee, who said that psychographic profiling is incredibly useful and not for the faint of heart.

Mr. Wylie, we've identified illegal conduct, I think, or potentially illegal conduct in relation to Brexit and spending. We've talked about AIQ's role, and they knew at the time that any overspending of a 7-million pound limit would have caused problems for Vote Leave, yet they funnelled money to other organizations. We know from testimony at the U.K. committee, from what I understand, that the same custom audiences were uploaded for both the BeLeave campaigns and the Vote Leave campaigns, yet AIQ had told us that no, the information was provided by the respective campaigns, which quite clearly is now a lie. That's potentially illegal conduct.

We have potentially illegal conduct or at least contrary to PIPEDA when Facebook shared, overshared information, potentially even private messages to Kogan, and Kogan then potentially improperly or illegally passed that on to Cambridge Analytica.

Are there other examples of potentially illegal conduct this committee should be seized with or be aware of?

Mr. Christopher Wylie: Is it in relation to Cambridge Analytica or just generally?

Mr. Nathaniel Erskine-Smith: To your knowledge, I mean, we're talking 600,000 Canadians who have been affected by just the Facebook to Kogan transfer, and that's not any other app. AIQ had an app on Facebook itself, and we don't know how much information was gleaned from that.

If we identify the players in this story, AIQ, SCL, and Cambridge Analytica, and you've worked for a fairly long period of time for Cambridge Analytica in a significant role as research director, from what you have seen, is there other illegal conduct in this story that we should be aware of?

Mr. Christopher Wylie: There may be, but I'm also aware that there are currently investigations going on, in which imparting that information in a political forum may interfere with a particular investigation. If you'd like to discuss that in a non-public forum then perhaps we could have a discussion.

Mr. Nathaniel Erskine-Smith: Perhaps, Chair, we can discuss this after the second round but potentially go in camera at some point.

We talk about profiling and political ads or companies advertised to in a targeted way. I think you've been right to highlight the difference between ethical and unethical uses of data and that it's perfectly acceptable to target some messages to certain people who may be interested in receiving that message. We know political parties do this all the time. In the last election the Conservative Party targeted Punjabi and Chinese communities to say that our Prime Minister wanted to open up neighbourhood brothels and sell marijuana to kids, so we know this happens.

The issue is scale and reach. When we talk about what the Internet's done and the understanding of the Facebook example of 87 million profiles being improperly shared, it's just an incredible scale that we haven't yet had to grapple with when it comes to targeting. When we talk about custom audiences, we can now not just reach communities through particular papers or particular interests —say this person likes animals or this person likes baseball— but we can now actually upload a custom audience and specifically get at these people.

So when we look at answers to this problem, I've read your article, "This is how Facebook can save itself", which begins with, "Rather than #DeleteFacebook, we need to #FixFacebook", and you talked about transparency. Perhaps you could speak to some solutions that this committee ought to be looking at, given your expertise.

Mr. Christopher Wylie: The first thing I would say is that I am not on a crusade against Facebook. I think there's a lot of really amazing things that Facebook does. The only thing I would say is that although a lot of attention has been put on Facebook, there are other social media companies that collect just as much data, or in some cases more data.

When we look at how society is moving forward, this is a one-directional movement, right? Every single year, we are integrating smart devices that are connected to algorithms, that are connected to databases, in new and multifarious aspects of our lives. People are putting Alexa into their homes. Their fridges can connect to their phones. We might have self-driving cars at some point in the future. With the advent of things like facial recognition or smart buildings, physical spaces at some point may be adapting themselves to your presence in them.

There are a lot of benefits to that, but there are a lot of risks. One of the things that I think should be considered is more rules on transparency for targeting. Currently, if you as a politician go out and do a constituency event, the media might show up, there's an audience, your opponent might show up, and if you tell an untruth you can be called out on that, right? Or, if you say something and there's a different perspective, there is some kind of accountability mechanism there. That is the essence of the public forum.

The problem with targeting is that rather than standing in that public forum, you are going to each individual voter and whispering something in their ear. Now, in many cases what you're whispering is something you would be happy to say in that public forum. In some cases, it may not be.

Currently—

● (1025)

Mr. Nathaniel Erskine-Smith: How narrow is the custom audience? To that point about whispering in one person's ear, custom audiences can be drilled down to what I can upload...a custom audience of one?

Mr. Christopher Wylie: Facebook limits the custom audience to 1,000—

Mr. Nathaniel Erskine-Smith: Okay.

Mr. Christopher Wylie: —but you could have 1,000 custom audiences of 1,000 to make up a million, and you have 1,000 different messages to a million people.

The point that I was going to make was that rather than say targeting is outright a bad thing and we shouldn't have it, there are really positive use cases, particularly with motivating under-represented groups in democracies to show up and vote. Simply requiring platforms like Facebook or Google or Twitter to publish every single ad that is being sent out on their platform would allow journalists, governments, parties, whomever, to look at what ads are on this platform and, in addition to that, the actual targeting specification for those adverts.

Currently, we do not know what goes on Facebook, on Google, on Twitter, in terms of targeted advertising, right? A simple solution to that would be to require those platforms to simply report what happens so there can be public scrutiny. In that way, you avoid necessarily creating a number of rules to restrict what you can and can't say on a platform, or having some cumbersome regulator. That would allow civil society and parties to scrutinize messaging in the same way they would if you were standing in that public forum. However, it would not prevent the really positive use cases of targeting, in particular engaging people who are under-represented in politics right now.

The Chair: Thank you, Mr. Erskine-Smith.

As a heads-up, we have bells at 10:56 a.m., and there's a vote at 11:26 a.m. That gives us another half an hour or so. We should be able to get back, but we're going to try to get through as much as we can.

Mr. Gourde, for five minutes.

[*Translation*]

Mr. Jacques Gourde: Thank you, Mr. Chair.

Mr. Wylie, I think it's noble to use technology to get out the vote. The problem arises when people are targeted so that they all vote for the same thing.

Why target certain people on Facebook, instead of just placing general ads, as is done in television, radio, newspapers, and other media?

[*English*]

Mr. Christopher Wylie: It's because young people, for example, are highly mobile, and the address on the electoral register is not necessarily where they live. They don't necessarily listen to the radio, and there is something to be said for sending messages to voters that contain a policy or issue that they actually care about.

If I'm in Nova Scotia, I may not be entirely concerned with wheat and farming policies in Saskatchewan, because what affects me is fisheries or something else. Targeting doesn't necessarily have to be a bad thing. You can have targeting that is positive for democracy because you are speaking to voters about something they actually care about, and indeed in a medium they actually see and engage with.

We have a declining turnout, and this is not just a problem in Canada. It's a problem all over the place, and it's because the media landscape has completely changed. Part of the job of political parties in maintaining our democratic process is to adapt to that new environment and to develop ways of engaging voters in that new environment. Digital has to be part of that. If we do not have digital communications in an increasingly digitized society, we are going to dramatically affect the results of elections towards people who aren't online, which is a vastly shrinking population.

We shouldn't necessarily treat social media or online communication as a bad thing. Just in the same way that a knife can be a murder weapon or create a Michelin star meal, it's a tool. The appropriate thing is to look at what is reasonable for this tool, work out how to use it, and create boundaries for it.

● (1030)

[*Translation*]

Mr. Jacques Gourde: Mr. Wylie, have you put a number, percentage-wise, on how much this technology increases voter turnout? Is it 2%, 3%, 4%, 5%, or 6% more people who vote?

[*English*]

Mr. Christopher Wylie: I can't give you a precise figure, but I recall seeing results that ranged from 2% to 7% in terms of uplift, which is not insignificant. If parties actually focused more on online engagement, they could actually increase turnout overall, but it's the job of all parties to do that for all of their own supporters and voters.

[*Translation*]

Mr. Jacques Gourde: Pollsters are having a harder and harder time predicting elections. In the last 10 days of an election campaign, major changes in how people are likely to vote can be observed. In fact, that's what we are seeing in Ontario, right now.

In the last 10 days of an election campaign, can these technologies have a huge influence by getting people who would not normally vote out to the polls?

[*English*]

Mr. Christopher Wylie: Pollsters have a hard time predicting, because they don't actually do forecasting. All they do is report the results of 1,000 people and what they said. Very little analysis actually goes into it in terms of creating forecasting algorithms or anything prospective. That's one of the reasons polling has become drastically inaccurate in a lot of places.

In terms of the impacts of targeting, it absolutely could affect the results of an election 10 days out. That's not necessarily a bad thing, but more parties and political actors should be looking at that problem and at ways they can engage people on digital platforms. More turnout is a good thing.

The Chair: Thank you, Mr. Gourde.

Next up, for five minutes, is Madam Fortier.

[*Translation*]

Mrs. Mona Fortier (Ottawa—Vanier, Lib.): Mr. Wylie, thank you very much for contributing to our study today. Your input is extremely important.

We've heard a lot about what went on. I would like to focus, however, on the future and talk about transformation.

A few times, you said that steps had to be taken to protect the personal information of Canadians. Do you have any such measures to suggest to the committee?

[*English*]

Mr. Christopher Wylie: The first thing—and this is a really straightforward example that I was speaking about before—is that, in the same way that you require transparency for donations and spending, you should require transparency for the use of information and advertising. When a party puts out an ad online, it should have to report that. It should also have to report who it is going to.

Personally, I think that companies should do that, too. I don't see why not. I think it would be healthy for people to be able to scrutinize the advertising markets online, in general.

The other thing is that we have to understand that this is not always going to be a data issue. The developments of algorithms and artificial intelligence moving forward means that it will not always be clear whether or not there was consent in an inference, for example. I will give you a tangible example. Your cousin joins a genetic-profiling company, like 23andMe for example. That company is acquired later by an insurance company or some other kind of company that looks at that genetic profile and infers, based on your relationship—because you're their cousin—that you have a 95% chance of having a particular type of breast cancer, and then denies health insurance. This might not be as applicable in Canada, but it absolutely is in the United States.

Here, there was consent in the actual data, because the data was the genetic profile of your cousin who consented to that use. However, the behaviour or action or result applies to you, where you didn't know that this was happening and you didn't consent to that.

Currently, it's difficult to say whether that information was about you. Was that an inference about you? When we're looking at artificial intelligence, we're looking at memories, understandings, behaviours, and inferences.

In the law, when we regulate people about their behaviour, we do have a component as to what's in their heads, but we also have another component, which is their behaviour. Taking a step back and not just looking at the issue of data and consent, but looking at the behaviour and acceptable behaviour of AI in general, is a really healthy mindset for people to have, I think.

These are decision-making machines, so we should be regulating how they can make decisions. This is really important because as society moves forward, all of this information is going to start being connected to each other. What you do with your toaster may affect what your office computer does later down the road, or it may affect the price of Starbucks, when you walk into Starbucks.

There are real issues that aren't to do with consent, but are to do with the ultimate impact in behaviour. That's a more broad mindset.

The third thing is that when you look at technology—whether you're a Canadian, an American, or a Brit, or whoever—the Internet is here to stay. You do not have a choice. You have to use Google. You have to use social media. You cannot get a job anymore if you refuse to use the Internet. This means that the issue of consent is slightly moot. In the same way that we all have to use electricity...it's a false choice to say that if you don't want to be electrocuted, don't use electricity. In the same way, if you don't want to participate in the modern economy, don't use data collection platforms.

We should be looking at these platforms as a utility in the same way that we would look at electricity, water, or roads as a utility, rather than as an entity where people or consumers are "consenting".

The fourth thing is that there should be rules on reasonable expectations. When I joined Facebook in 2007, it did not have facial profiling algorithms. I put all of my photos onto Facebook, and I consent to "analysis of the data that I put on", but that technology did not yet exist. Facebook then creates facial recognition algorithms that read my face. Was that reasonably expected at that time? For a lot of people, it probably was not. There's very little regulation or rules on something that's very unique to technology, which is the rapid development of new things.

● (1035)

Having some sort of rule or principle about reasonable expectation.... You might have consented to some platforms several years ago, but if something new happened, was that reasonably expected? If the answer is "no", then maybe it shouldn't be allowed.

● (1040)

The Chair: Thank you.

Next up, for five minutes, is Mr. Kent.

Hon. Peter Kent: Thank you, Mr. Wylie. Your recommendations in terms of every political party advertising that it has micro-targeted in elections is a good one, and I suspect that the commissioner, on receiving that sort of advice, may well come back and recommend it himself.

When Chris Vickery, director of cyber-risk research at UpGuard, testified before this committee, he described his accidental discovery of the public website called GitHub, the subdomain called GitLab, and the website gitlab.aggregateiq.com, which he said was essentially inviting the entire world to log on to register and participate in what he called a collaboration portal.

Do you think that the portal was left open deliberately by AIQ so that the company, or individuals in the company, could have plausible deniability of what was going on within areas of that portal?

Mr. Christopher Wylie: I can't speak to the intentions of AIQ, so I don't know why that misconfiguration was there. It seems like it was a pretty careless—which is one word you could use—oversight, to have their entire code base and systems exposed to the public. If not intentional, it certainly was extremely reckless.

Hon. Peter Kent: Did you ever avail yourself of the open accessibility of that site? Were you aware of it?

Mr. Christopher Wylie: I've used GitHub, as most people in tech have used GitHub, but this particular subdomain that you're referring to, I have not accessed before, no.

Hon. Peter Kent: Were you aware of GitLab-AIQ's Ephemeral project?

To be more specific, Chris Vickery walked us through the Ephemeral project, as he discovered it. That site has been taken down, but it had within it something called the database of truth, and then it had two different project levels to influence election outcomes. One was called Saga and one was called Monarch. Were you familiar with these projects?

Mr. Christopher Wylie: I am vaguely familiar with the names, actually through Chris Vickery, because those weren't necessarily the names that SCL would use to refer to the products. It's hard for me to answer specifically, because I am familiar with the general set-up. For example, for the "database of truth" that you're referring to, the parlance I used was the "database of records". I am familiar generally with the set-up, but I'm not familiar with the specific names off the top of my head.

Hon. Peter Kent: I know there is good humour among those who are experts in the digital world, but the subtitle of the Ephemeral project on this website was, "Because there is no truth." Do you think that was just a bit of humour, or more of an underlying reflection of the mentality of AIQ?

Mr. Christopher Wylie: I can't speak to the specific intentions of AIQ and why they put certain things there, but there was a systemic culture in the group of companies that we've been speaking about that completely disregarded the importance of truth in an election. SCL and Cambridge Analytica regularly advertised disinformation as a service offering.

Part of it could be dark humour, and part of it could also be reflective of the fact that this kind of humour would be completely acceptable in this group of companies.

The Chair: Thank you.

Next up, for five minutes, is Mr. Baylis.

Mr. Frank Baylis: I'd like to continue with our discussions about the foundations of Cambridge Analytica. What was the intention in setting up Cambridge Analytica?

● (1045)

Mr. Christopher Wylie: Robert Mercer and Steve Bannon wanted to use the services of SCL, but there were two issues. First of all, there were issues in the United States about using a foreign contractor, particularly a foreign military contractor, in domestic U. S. elections. This was in both a compliance sense—that's not allowed—and secondly an optics sense—that doesn't look good. They needed a domestic U.S.-focused brand for that operation.

Secondly, Rob Mercer wanted more control over the project than simply handing it to a client would allow. He wanted a role as an investor and as a shareholder and as a director.

Mr. Frank Baylis: He put Steve Bannon there as the vice-president.

Mr. Christopher Wylie: Yes.

Mr. Frank Baylis: Was it your understanding that he was doing this for a profit motive?

Mr. Christopher Wylie: Actually, no; the opposite. You have to remember that Robert Mercer is one of the wealthiest people in the United States. He's a billionaire. He doesn't need more money. The contract values you get in politics pale in comparison with corporate finance. For him, he wasn't necessarily out to make money, particularly, on political projects. He was out to play the sport of billionaires, which is to compete in elections.

Mr. Frank Baylis: In fact, this company was so poorly run it went bankrupt, right ?

Mr. Christopher Wylie: Yes.

Mr. Frank Baylis: So we can look at it and say that he didn't do it for financial profit.

Now, let's say I set up a sign company here in Canada and say to a given party, "I'm going to sell you your political signs at a discount. I'm going to lose money. I'm a rich person and I want to 'subsidize' selling the election signs you're going to stick up. I'm selling them under price."

So I'm actually giving money indirectly, which is against the law.

Mr. Christopher Wylie: Yes.

Mr. Frank Baylis: Is it possible that Steve Bannon and Robert Mercer, in the structure they had in this money-losing operation, were also circumventing election spending limits—or election spending laws, if you will?

Mr. Christopher Wylie: So one of the ancillary benefits.... I can't speak to the specific intention or to the reason it was set up this way. I mean, it was set up with an incredibly convoluted structure, but as it was explained to me, there is a benefit. That is, if you are an investor in a company that then provides political services, and you put money into that company that then provides services at a particular rate, then when you put money into that company, that's not a donation. That's an investment in a company that you're the owner of. In that way, it doesn't necessarily need to be reportable, because it's an investment.

If you are then putting in millions and millions and millions of dollars to generate IP, which is then worth millions and millions and millions of dollars, but you then only need to charge your clients a nominal amount, you could argue that this is a subsidy. You could argue that it's a donation in kind, or that it's a proxy donation. The problem in many cases in the United States is that companies are much more opaque than in other countries, so it's difficult to actually parse out how much money goes where.

So that was explained to me as an ancillary benefit.

Mr. Frank Baylis: Given the fact that they also had their hands in the Brexit vote, it could also be a way of them...of a foreign entity pushing money into another country's domestic vote, through Brexit. Could you speak to that?

Mr. Christopher Wylie: Yes. I think this is in part where a vulnerability has been exposed in a lot of countries' electoral laws. If you pass money into companies, and then those companies provide services for domestic clients, it's not always transparent where some of that money came from. More reporting mechanisms for companies that do engage in politics would be something to explore.

● (1050)

Mr. Frank Baylis: Thank you.

The Chair: The last question goes to Mr. Angus, for three minutes.

Mr. Charlie Angus: We've received a number of questions from citizens through OpenMedia. Many of them, I think, are questioning the bigger issues in terms of regulation and how we start to move towards what you call dealing with these tech giants, these utilities. I think one of the questions is staring us in the face. That is, how likely it is that Cambridge Analytica and SCL were the lone operators in this big field of election manipulation? Were there, and are there, other players out there that we should be aware of?

Mr. Christopher Wylie: The way I look at it is, Cambridge Analytica is the canary in the coal mine. Cambridge Analytica is the beginning; it's not the end. What CA has exposed is how easy it is to misappropriate information, take funds from mysterious sources, and then go and interfere in elections, particularly in cyberspace. What it really shows is how the Internet and the growing digitization of society have opened up vulnerabilities in our election system.

Elections, historically, feel like a very domestic, insulated activity, because previously, if you were a foreign actor, you would have to physically come to a country to interfere. Now you don't. I think, moving forward, we need to look at cybersecurity as a priority for elections, and we have to understand that we may look at social media as domestic political players, as a communication space, as scoring points, or for messaging.

If you are a malicious foreign actor, you look at it as an information battlefield. You don't look at these people as voters; you look at them very much as targets for manipulation and targets for division. This is why transparency mechanisms or requirements for online platforms that do any advertising in the political space would be a really helpful first step. That would make it a lot more difficult for a country like Russia to start to interfere in elections, if it has to be done in public.

Mr. Charlie Angus: It would be really helpful if you could send our committee some recommendations that we should be looking at. What really struck me was, when we had Facebook here, they seemed to have a very cavalier disregard for the damage that was done through the manipulation of their platform. I see Facebook as having a revolutionary, positive potential. Certainly in my region, it's been transformative in connecting isolated indigenous communities. When we asked questions on, for example, the horrific ethnic slaughter in Myanmar and Facebook's unwillingness to police its own network or to deal with the calls from UN NGOs, they shrugged.

How do we come up with better mechanisms to protect democratic elections and to respond to this kind of misuse of platforms by these third-party operators?

Mr. Christopher Wylie: I think one of the biggest things that I've learned in this process is that I get a lot of the same questions and see a lot of the same problems with the different legislators and governments that I've been dealing with around the world. One of the things that I've also seen is how Mark Zuckerberg, for example, refuses to appear at any of the other committees or investigations around world, save for Congress and his very brief meeting, if you can call it that, at the European Parliament. This means that you've got largely American companies that are exerting huge amounts of influence on the democratic systems of countries all around the world.

I think a starting point would be different legislatures, different regulators, and different governments sitting down together and talking about how it is that the Internet is global and everybody has a stake in making sure that their democracies are intact. What is it about the Internet that needs to be looked at? What are the common questions that each country has? They should be working together on a common solution. I honestly think that it may require a multinational approach, particularly when you see how Mark Zuckerberg refuses to engage with most countries.

Mr. Charlie Angus: But domestically—

Mr. Christopher Wylie: I think that it has to happen at an international level or across parliamentary level.

Mr. Charlie Angus: Finally, domestically, would you say that it would be in Canadians' interests to have Canadian political parties come under our privacy protection act so that there is more accountability for how political parties use this information?

● (1055)

Mr. Christopher Wylie: The only issue that I think would need to really be carefully considered is, if you start to require political parties to have opt-in consent before they talk to voters, or if they receive some kind of opt-out, they can never engage that voter again, and you may create a situation where you have an election and you are unable to reach the entire electorate because of those barriers.

Our democratic process is a very special thing, and I think that there is value, sometimes, in one party approaching a voter who doesn't initially agree with them or doesn't even necessarily want to talk to them, because that's partly what debate and the political process is about; it's about challenging conversations. You can't have challenging conversations if we create rules that prevent political parties from engaging with the voters.

It's different for companies than with elections, but in particular with elections, I think that's a really important thing for people to think about, that it feels good to say we should have opt-in. If you don't want to talk to parties, they shouldn't have to bother you at the door, but sometimes, that's essential in maintaining our democratic process.

The only caution that I have there is just making sure that it's not so overly restrictive that five years down the road, parties can't engage with the electorate.

The Chair: Thank you.

I have a question for you, Mr. Wylie. I have a couple, actually.

We have to go to votes here in a few minutes. Are you able to stay to answer a few questions in camera when we come back?

Mr. Christopher Wylie: Sure. I'm not sure what time it is at the moment, but I'm sure I can, yes.

The Chair: We've already checked, and the building that you're in is going to be open to you, to be accessible to us, at least until 12:45 p.m. That already has been worked out, so you're free to stay.

Mr. Christopher Wylie: Sure.

The Chair: Okay, I have a question for you, as chair, and then we're going to go to votes and then come back. We'll come back in camera.

Have you watched the testimony of Mr. Zack Massingham and Mr. Jeff Silvester when they appeared before our committee in Canada?

Mr. Christopher Wylie: I've watched parts of it. I haven't seen the entire thing.

The Chair: Okay. Is it your opinion, in watching that testimony, that they were untruthful to our committee?

Mr. Christopher Wylie: My impression was that there were answers that felt obfuscated or that were, as has been discussed now, so fantastical that they're hard to believe.

The Chair: Okay.

Could we have unanimous consent to continue for about one minute, and then we'll come back in camera? Okay.

Thank you for your testimony, Mr. Wylie. We trust that you'll be back when we come back. We're going to be back around 11:45. You can go and come back—that's fine.

As for the committee, we're going to be coming back to ask questions in camera. Is that clear, everybody?

We'll suspend just for a few minutes, and we'll see you when we get back, Mr. Wylie.

Thank you.

[Proceedings continue in camera]

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: http://www.ourcommons.ca

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : http://www.noscommunes.ca